APPLICATION OF ARTIFICIAL NEURAL NETWORKS FOR THE DETECTION OF TELECOMMUNICATION FRAUD

ASOGWA E. C[1], OKOLO C. C[2], EZEUGBOR I. C[1], NGENE C. C[1]

1. DEPARTMENT OF COMPUTER SCIENCE,
NNAMDI AZIKIWE UNIVERSITY, AWKA,
ANAMBRA STATE

2. ELECTRONICS DEVELOPMENT INSTITUTE,
FEDERAL MIN. OF SCIENCE AND TECHNOLOGY
AWKA CAPITAL TERRITORY, ANAMBRA STATE

ABSTRACT

Neural computing refers to a pattern recognition methodology for machine learning. The resulting model from such neural computing is known as artificial neural network (ANN) or a neural network. The Neural networks can be used in so many applications in businesses for pattern recognition, prediction, forecasting and classification. The applications of artificial neural network based data mining tools are seen in information systems, marketing, finance, manufacturing and so on. The above discusses the role of artificial neural networks in detail to prevent telecommunication fraud which is presently causing some setbacks in the industry.

Keywords: Telecommunication fraud, Subscription, Artificial neural networks (ANNs), Data Mining, Expert System, Rule Based System

INTRODUCTION

In recent times, the telecommunication industries have recorded a lot of improvement considering the affordable mobile phone technology. The mobile phone fraud is recently on the rise globally and this is caused by the increase in the number of mobile phone subscribers. It is a worldwide problem that affects the annual revenue losses of many industries. Fraud detection is a discipline that requires an intelligent tool to adapt to the strategies of these fraudsters in committing fraud. Telecommunication fraud is profitable to fraudsters because the call they make is not restricted to a physical location and it makes things very easy for them to get a subscription illegally. It's established that with minimal investment and low risk of getting exposed, these fraudsters provides a means for illegal high profit business for themselves. Telecommunication fraud is stealing of telecommunication services. The victims of such fraud are businesses, consumers and communication service providers.

Telecommunication fraud is said to exist when telecommunications services are used with no intention to pay. This fraud has some attractive gain that makes it enticing to fraudsters. The problem with localization is small and simple custody of an access code, which can be obtained even through social engineering, makes the practice of this fraud feasible.

TELECOMMUNICATION FRAUD DETECTION

Telecommunication fraud is a very big loss in the company's revenue and can also affect the credibility and performance of telecommunication companies negatively especially with the known fact that fraud is dynamic. This means that this fraudster's always finds a way to thwart the security measures when they feel threatened or that they are being monitored. These frauds have increased rapidly to the extent that losses to telephone companies are checked to the tune of millions of naira. Fraud impacts negatively on the telephone companies in four (4) ways. These are as follows;

Financially

Marketing

Customer relations

Shareholder perceptions.

There are various techniques available for managing and detecting telephone fraud these include:

1) The Manual review of data. In this case, there are so many data records for the company to filter the fraudulent datas from such millions or more of records in a month. This record is also for a limited region only. The technique is time consuming for detecting fraud.

2) Conventional analysis using a fixed rule based expert system together with statistical analysis. A rule based system is a set of rules that take into account the normal calling hours, the called destinations as well as the normal duration of the call and etc.

3) Adaptive flexible techniques using advanced data analysis like artificial neural networks (ANNs). Fed with raw data, a neural network can quickly learn to pick up the patterns of unusual variations that may suggest traces of fraud on a particular account.

TYPES OF FRAUD

IDENTITY THEFT- This is the misuse of information that is personal in order to convince others that the imposter is the person. It’s the effectively passing of oneself off as someone else.

INTERNET FRAUD – This is any type of fraud that uses either one or more components of the internet such as email, chat rooms, websites etc to present fraudulent appeals to their prospective victims, to embark on fraudulent transactions or to transmit the financial gain from fraud to financial institutions or to others connected with the fraud.

TELEMARKETING FRAUD – This is a type of fraud whereby the person(s) carrying out the fraud will make use of the phone as a major communication means with prospective victims and move to persuade for money to be sent to them.

AUCTION AND RETAIL SCHEMES - These schemes attract consumers by purporting to offer high-value merchandise at attractive prices. After persuading the prospective victims to send money either in the form of a personal check, money order, or cashier's check. The fraudsters will either send inferior items or nothing at all.

NIGERIAN MONEY OFFER SCAMS – In this scheme, prospective victims receive, a request from a purported high ranking Nigerian government official either through e-mail or fax, seeking permission to transfer or move a large sum of money out of the country into the prospective victim's bank account.

ATM FRAUD - The magnetic strip on the back of credit and debit cards is secretly copied with a special information storage device. This happens during transactions such as an ATM withdrawal etc

INVESTMENT SCAMS- in this type, Market manipulation fraud has two methods the fraudster’s uses. They are as follows;

Pump and dump: this is observed when an attempt to illegally influence the price of some stocks of oil companies and sending such inflation out through e-mails.

Short-selling: in this method, the scammer decreases a stock value of a company.

TELECOMMUNICATION FRAUD- this is the type of fraud that affect the telecommunication section or companies. The fraudster manipulates the use of telecommunication to their gain and loss of the telecommunication companies.

TYPES OF TELECOMMUNICATION FRAUD

The two most types of telecommunication fraud are subscription fraud and superimposed fraud.

SUBSCRIPTION FRAUD: In this fraud, fraudsters always obtain an account even when they have no intention to pay for the subscription. In such a case, excessive usage of the phone subscription usage occurs throughout the period when the account is active. In most cases, such accounts are used either for call selling or intensive self usage.

SUPERIMPOSED FRAUD: In this fraud, fraudsters hijack a functional and legitimate account of a subscriber to use for fraudulent activities which in most cases are excessive usage. This can be done by cloning the mobile phone and also obtaining the calling card authorization details.

METHODS OF TELECOMMUNICATION FRAUD

The methods are as follows;

THEFT ON COMMUNICATION SERVICES: The rate at which the telecommunications services are stolen lately is on the increase. Some seek to avoid or to get a discount on the actual cost of a phone call while some are illegal immigrants who couldn’t get legitimate information services without exposing their status.

COMMUNICATION IN FURTHERANCE OF CRIMINAL CONSPIRACIES: The fraudsters rely on information systems which helps them with communications and the keeping of record as much as legitimate.

LITERATURE REVIEW

Traditional fraud techniques are adapting to the network infrastructure of the recent times. The deceptions in the world of telecommunication include subscription frauds where the fraudster uses the services he or she didn’t subscribe. In some cases, the user can be charged for services used by fraudsters and this is called identity theft. These fraudsters who exceed their download quote, the rate illegal services redistribution for an economic profit can be identified by Telecommunication operators. Phone cloning or unauthorized access to services leads to compromising the customer privacy. Anyway the most common types of fraud on telecommunications are subscription fraud. Fraud management system is an appropriate tool to detect fraud with diverse techniques. The techniques are as follows;

Self organizing maps (SOM)

General data mining

Artificial intelligence techniques (Rule based systems profiling) like neural networks based on the hierarchical regime switching models, fuzzy rules, Bayesian networks or other data mining techniques.

Most of these techniques uses the CDR data to create a user profile and also detect irregularities based on the profiles. The large amounts of CDR help to find patterns and scenarios of normal usage and typical fraud situations. These scenarios are used to configure monitors that observe the behavior of the user with respect to the type of fraud. Then, the monitors are arranged in a neural network which activates an alarm as soon as fraud is noticed. Such system can be classified in a rule based approach knowing that abnormal usage triggers certain rules. Rules need to be specific to avoid false positive alarms. It also needs to always detect new scenarios which result in very time consuming programming. From the reviews, the most commonly used methods for fraud detection are signature based. These methods detect the fraud by considering the deviation detection. This comprises of the comparison between the recent activity and the user behavior data which is expressed through the user signature. This mentioned work can be adapted and extended by reformulating the notion of signature and by the existence of the notion of statistical based distances to detect irregularities in fault detection. When the simple statistical functions are used to avoid processing costly histograms, the computational cost can be reduced. Some other techniques like neural networks, have applied for fraud detection.

METHODOLOGY

USING ARTIFICIAL NEURAL NETWORKS TO DETECT TELECOMMUNICATION FRAUD

Many industries have been using the aid of Artificial intelligence technologies as fraud detection systems for so long. Falcon or credit card issuers which is a neural network that is based on fraud detection systems, is provided by Hecht Nielson Neuro-computers of San Diego, California. Coral Systems provides a knowledge oriented systems for cellular fraud detection in the telecommunication. The system has an expert fraud rules which it uses to identify possible fraudulent calls outside the actual pattern of a caller activities. A caller that does phone calls in a rapid succession possibly has the phone cloned and that is a common practice among these cellular fraudsters for stealing and using a legitimate cellular accounts. If a caller that makes an average of 45 calls per day and later starts making up to 50 calls, no fraud alert will be activated. But when a different caller that makes only few calls per week suddenly makes up to 50 per day, the account will be activated for fraud investigation. The system will pull the information in the carrier switches to search for a deviation from a caller's normal patterns of phone usage. The system can be programmed to give alerts for any suspicious call or can also be programmed to provide as few false positives as possible, which increase the rate of the fraud among flagged calls to 90-95% but it may omit many frauds. The systems have been out since 1992 and according to Coral systems are in use by 5 customers. While this system does not currently use neural networks Coral is investigating them for future use.

An overview of the Fraud Detection System developed by using Artificial Neural Network Technology is shown in the below figure: The process begins with gathering historical data on fraudulent and non fraudulent calls. This data is preprocessed to make it suitable for neural network learning. Next the neural network is trained using the preprocessed data to build a model which incorporates numerous patterns of fraudulent behavior. The model is applied to incoming business where it adaptively learns new patterns of fraud improving its model as the types of fraud evolves. Fraud detection mechanisms may be home brew, proprietary or a mix of both which is probably the healthiest approach. A web search for telecom fraud management will result in a bewildering number of hits. Simple thresholding systems work well when integrated into business as usual processes and could well account for 80% or so of the fraud management load. For more complex situations where product interaction is taking place, some form of correlation is required using neural or artificial intelligence techniques. One should also consider the near real time nature of emerging frauds and the need to close down potential high cost fraud quickly. Globally the usual experience is that fraud management system pays for their investment in very short times provided they are directed at the principal sources of fraud. Data sources for fraud detection systems are principally Call Detail Record (CDR) based, deriving usually from the host billing system. For a more real time data source the

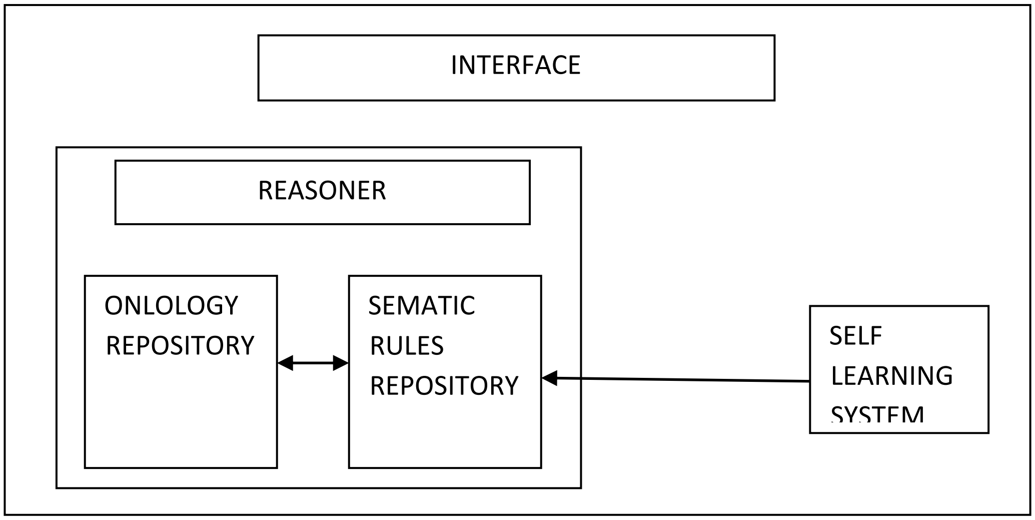

Fig. 1. Fraud Detection System using ANN Technology Source

In the narrowband world this will mean monitoring Number 7 signaling messages at strategic points in the network. Network topology then becomes an issue. In a network with widespread use of Signal Transfer Point (STP) working, signaling is concentrated in a relatively few points and monitoring may be economically infeasible so a more focused approach is called for. PSTN itself is the usual source. The usual axiom is to follow the money. Therefore monitoring international routes would be a priority. One could also consider monitoring the Intelligent Network platform as this usually provides a signaling concentration point and may also deal with high value number translation services such as Premium Rate. As voice over IP services roll out, fraud detection system manufacturers are turning their attention to the specific needs of extracting or creating CDR’s from telephony services or other network components. The fraud detection mechanism consists of a rule based system for detecting fraud and a self learning system that makes this system adaptive. A rule based tool was a white box approach that allowed detecting the frauds with low rate or false alarms. More specifically the rule based system contains an ontology repository which is practically the knowledge base of the system and which stores all the domain and fraud specific knowledge that is required by the system. The actual fraud detection methods and techniques are stored in the Semantic Rules Repository in the form of if-then-else rules that reason over the knowledge contained in the ontology repository. The two repositories are interrelated as the representation of rules depends on the contents of the ontology. Finally the self learning system provides the overall system with the capability to learn new rules about fraud from the submission of fraudulent and non fraudulent domain specific data and to automatically detect irregular observations in the data thus providing a feedback mechanism for enriching and updating the repository of rules. The self learning system integrates suitable algorithms for statistical data analysis and data mining tasks that enable it to update, optimize and extend existing fraud detection rules by analyzing submitted data. The fraud detection area is an active area of development for neural networks in telecommunications. Many of the most successful systems are hybrid systems which takes advantage of the relative strengths of several Artificial Intelligent technologies. Given the payoffs involved it is an application which should come into routine use in the years ahead.

RESULTS AND ANALYSIS

The Forum of International Irregular Network Access (FIINA) earlier estimated that the telecommunication fraud result is in a loss of United States $55 billion per year worldwide. South Africa’s largest telecom operator was losing over United States $37 million per year to fraud. Subscription fraud in which a customer either provides fraudulent details or gives valid details and then disappears was the company’s biggest cause of revenue leakage. By the time the telecom provider is alerted about the fraud, the fraudster has already moved to other target victims. Other types of fraud include phone card manipulation which involves tampering and cloning of phone cards. In a clip on fraud a fraudster clips on to customers telephone lines and then sells calls to overseas destination for a fraction of normal rates. Minotaur, developed by Neural Technologies was implemented to prevent fraud. minotaur uses a hybrid mixture of intelligent systems and traditional computing techniques to provide customer subscription and real time call monitoring fraud detection. This assists in processing the data from this numerous fields using a multi-stream analysis capacity. Frauds are detected on several levels such as on an individual basis using specific knowledge about the subscriber’s usage and on a global basis using generic knowledge about subscriber usage and known fraud patterns. In the first three months of installation of this neural network based software: The average fraud loss per case was reduced by 40%. and The detection time was reduced by 83%.. The combination of neural, rule based and case based technologies provide a fraud detection rate superior to that of conventional systems. Furthermore the multi stream analysis capability makes it extremely accurate.

CONCLUSION

The theft of telecommunication services has been one of the most enduring types of telecommunications fraud that have been in existence since the inception of telephone systems. A research on the fraud detection in the mobile telecommunications is a recent development. Other works in the area of fraud detection in phone telecommunications are based on data mining approaches. Due to its characteristics this type of fraud requires real time and individualized customer analysis. Each technological development designed to thwart criminal endeavors has been quickly followed by the creation of a new form of crime designed to exploit new security. These few directions of future policy may assist in ensuring that the full potential of global telecommunications developments will be realized while at the same time providing both service providers and users with some expectations that their property rights will be respected. Fraud detection will continue their accelerated use of neural network based systems. Many of the laboratory techniques for using neural networks in metro burst communications, satellite network management and traffic control will come on line. In short the neural networks will become an increasing presence in major aspects of telecommunication networks improving efficiency, adapting to changing calling patterns, and providing better information about the use of networks. Neural networks a technology which has been used in telephony since the early 1960s is beginning to make it presence felt in designing in telecommunications network of the next century. As a result Artificial Neural Network is a better method for detecting telephone fraud, due to its inherent ability to adapt as well as its speed and efficiency.

ACKNOWLEDGMENT

I am heartily thankful to my Dean Dr. Faisal Bugdadi and head of the Department, Mr. Abdulwahab Alamri, who encouraged me to prepare this paper. I am also thankful to my colleagues and friends for their support. Any suggestions to further improvement of this topic are most welcome.

REFERENCES

[1] Pieprzyk J, Ghodosi H and Dawson E (2007), Information security and privacy: 12th Australasian conference, ACISP 2007, Townsville, Australia, July 2-4, 2007: proceedings, Springer, Germany, pp 446-447.

[2] Liatsis P (2002), Recent trends in multimedia information processing: World Scientific Publishing, London, pp 474-475.

[3] Prasad S K, Routray S and Khurana R (2019), Information Systems, Technology and Management: pp 259-260.

[4] Żytkow J M and Rauch J (1999), Principles of data mining and knowledge discovery: Third European Conference, PKDD'99, Prague, Czech Republic, September 15-18, 1999 : proceedings, Springer, USA, pp 251.

[5] Wall D S (2016), Crime and the Internet, Routledge, London, pp 30.

[6] Broadhurst R G and Grabosky P N (2005), Cyber-crime: the challenge in Asia, Hong Kong University Press, Hong Kong, pp 32.

[7] Samarati P (2010), Information Security Theory and Practices: Security and Privacy of Pervasive Systems and Smart Devices: 4th IFIP WG 11.2 International Workshop, WISTP 2018, Passau, Germany, April 12-14, 2018, Proceedings, Springer, USA, pp 201.

[8] Perner P (2006), Advances in data mining: July 16-17, 2019 : proceedings, Springer, Germany, pp 535.